Exam.Code:0923
Sub. Code: 33551

2076

B.E. (Information Technology)

Fifth Semester

PCIT-501: Network Security and Cryptography

Time allowed: 3 Hours

Max. Marks: 50

NOTE: Attempt five questions in all, including Question No. I which is compulsory and selecting two questions from each Section.

x-x-x

1	a)	Define CIA Triad and explain how the compromise of any one of its components can affect the security of an information system.	2
	b)	Differentiate between symmetric and asymmetric cryptography. Which technique is more suitable for secure key exchange? Justify your answer.	2
	c)	What is the purpose of a Message Authentication Code (MAC)? How does it differ from a digital signature in ensuring message integrity?	2
	d)	State any two characteristics of a firewall. Why is a firewall alone not sufficient to secure an organization's network?	2
	e)	What is SQL Injection? Explain how prepared statements (parameterized queries) help prevent SQL Injection attacks.	2

Section - A

2	a)	An organization wants to ensure confidentiality, integrity, authentication, and non-repudiation for its network communication. Explain which security services and security mechanisms of the OSI Security Architecture should be employed to achieve these objectives.	5
	b)	Encrypt the plaintext "INFORMATION" using: i) Caesar Cipher with key=4, ii) Columnar Transposition Cipher using the key "3142" Show all intermediate steps and compare the characteristics of substitution and transposition ciphers based on the obtained ciphertexts.	5
3	a)	Explain the working of the Data Encryption Standard (DES) with a neat block diagram. Why has DES become unsuitable for securing modern communication systems? Justify your answer.	5
		Describe the working of the Advanced Encryption Standard (AES) algorithm. Compare AES and DES with respect to key size, block size, security, number of rounds, and performance.	5

P.T.O.

4 a) Write the Diffie–Hellman Key Exchange algorithm. Using the following parameters, determine the public keys and the shared secret key established between Alice and Bob: p=23, g=5, Alice's private key, a=6, Bob's private key, b=15 Show all intermediate calculations and verify that both users obtain the same shared secret key. 7

b) An organization has 20 users communicating through a symmetric key cryptosystem. Determine the number of secret keys required for secure communication among all users. Briefly explain why key distribution becomes difficult as the number of users increases and suggest a suitable solution. 3

Section -B

5 a) Explain the IPSec architecture with a neat diagram. Discuss the role of Authentication Header (AH) and Encapsulating Security Payload (ESP) in providing security services for IP communication. 5

b) An e-commerce company wants to secure customer transactions over the Internet. Explain the working of the SSL/TLS protocol with a neat diagram and justify why SSL/TLS is preferred over transmitting data without encryption. 5

6 Write the RSA algorithm for key generation, encryption, and decryption. Using the RSA algorithm, perform key generation, encryption, and decryption for the following parameters: p=11, q=13, e=7, and M=9. Determine public and private keys, ciphertext generated after encryption, and original plaintext obtained after decryption. Verify that the decrypted plaintext matches the original message. 10

7 a) Explain intrusion detection systems (IDS). Compare Host-based IDS and Network-based IDS. 5

b) Discuss any five common web security attacks and suitable countermeasures. 5

x-x-x